III. REMARKS

1.   Claims 1, 8, 15, 19, 26 and 32 are amended. Claims 1-35 are pending in the Application.

2.   Claims 1-7, 15-25 and 32-35 are patentable under 35 U.S.C. 102(a/e) over Sudia, U.S. Patent No. 5,841,865. Claim 1 recites an input element for receiving from a selected device a request that is generated upon initial power up of the selected device, for configuration of the selected device from a generic configuration to a selected or custom configuration through the communications network, the request including coded information. Claim 1 further recites a processor responsive to the request for locating a record associated with the selected device, and verifying an identity of the selected device based on the coded information, the record including second information concerning the selected or custom configuration for the selected device, the selected or custom configuration corresponding to a predetermined feature set of the selected device. Sudia does not disclose or suggest a request that is generated upon <u>initial power up</u> of the selected device, for <u>configuration</u> of the selected device from <u>a generic configuration to a selected or custom configuration</u> or that the selected or custom configuration corresponds to a <u>predetermined feature set</u> of the selected device.

Sudia discloses a cryptographic key escrow system and public key certificate management enforced by a self-certifying chip device relating to the secure generation, certification, storage and distribution of cryptographic keys used in cryptographic communications systems (Col. 1, L. 15-23). The manufacture of the trusted device in Sudia is based on (1) an embedded microprocessor and miniature computer, (2) an optional

10

cryptographic coprocessor which can perform standard mathematical encrypting and decrypting operation, (3) an input-output interface or subsystem to assist in handling the flow of data commands to and from the microprocessor, and (4) a memory subsystem that may potentially employ several types of memory storage technology (Col. 13, L. 34-65). Sudia also discloses a tamper-resistant trusted device that can upgrade or supplement in a trusted manner any firmware routines embedded by the manufacturer. The trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code that is suitable for that type of device and is digitally signed with the manufacturer's signature (Col. 39, L. 7-20). This however is not what is claimed by Applicant's claim 1.

Claim 1 recites an input element for receiving from a selected device a request that is generated <u>upon initial power</u> up of the selected device, for configuration of the selected device from a <u>generic configuration to a selected or custom configuration</u> through the communications network, the request including coded information . . . the selected or custom configuration corresponding to a <u>predetermined feature set</u> of the selected device. Sudia discloses a trusted device with an input-output interface or subsystem to assist in handling the flow of data commands to and from the microprocessor (Col. 13, L. 49-51) and that the trusted device can upgrade or supplement manufacturer embedded firmware (Col. 39, L. 7-9). Nowhere does Sudia disclose the trusted device making a <u>request that is generated upon initial power up</u> for an upgrade or supplement of the firmware in the trusted device from a <u>generic configuration to a selected or custom configuration</u>.

The Examiner takes official notice "that the request is automatically generated on an initial power up of the apparatus because the sender cryptographic device uses an algorithm to encrypt the message when loaded with the cipher key for the session of communication" (as recited at Col. 2, L. 3-6 of Sudia). However, there is no basis in this passage or any other passage of Sudia for the Examiner taking official notice that the request is generated on an initial power up of the apparatus. Column 2, lines 3-6 of Sudia merely refer to the encryption of a message between two cryptographic devices using symmetric key algorithms and nothing more. In addition, Sudia discloses that in symmetric key cryptosystems there is a need for the sender and the recipient to exchange the cipher key over a secure channel to which no unauthorized third party has access, in advance of the desired communications between the sender and the recipient (Col. 2, L. 9-15). This process of first securely exchanging cipher keys and only then encrypting the communication is unworkable in situations requiring spontaneous or unsolicited communications (Col. 2, L. 15-18). Thus, the Examiner's taking of official notice is contrary to the teachings of Sudia and to what is claimed in claim 1. A request that is generated upon initial power up is a spontaneous or unsolicited communication because the server and the selected device are not in prior communication and the server does not know such a request is coming. Nowhere can it be inferred that any of the encryption in Sudia is performed upon an initial power up of the cryptographic device or that a request is generated upon power up of the cryptographic device. It is requested that the Examiner provide a detailed basis for taking official notice that the request is generated upon initial power up.

Furthermore, Sudia does not disclose or suggest that the trusted device has a generic configuration that is modified from the generic configuration to the selected or custom configuration. Sudia merely discloses that the permanent and non-modifiable memory space [of the chip] contains data and firmware embedded into the chip during manufacturing (Col. 16, L. 14-16) and that the trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code (Col. 39, L. 7-20). There is simply no disclosure or suggestion that the manufacturer configuration of the chip in Sudia is generic or that the manufacturer configuration is modified to a selected or custom configuration.

In addition, claim 1 recites the record including second information concerning the selected or custom configuration for the selected device, the selected or custom configuration corresponding to a predetermined feature set of the selected device. In Sudia, the chip's memory is divided into at least three general areas. A permanent and non-modifiable memory space containing data and firmware embedded into the chip during manufacture. Semipermanent and modifiable memory space containing data, such as the user's private encryption and signatures keys and non-permanent and temporary memory space containing work area used for temporary storage of the inputs, intermediate results and final results of various data processing operation. (Col. 16, L. 12-32). Sudia simply does not disclose or suggest second information concerning the selected or custom configuration for the selected device, the selected or custom configuration corresponding to a predetermined feature set of the selected device. Therefore, claim 1 is patentable over Sudia.

13

Claims 15, 19 and 32 are patentable over Sudia for reasons similar to those described above with respect to claim 1. Claims 2-7, 16-18, 20-25 and 33-35 are patentable by reason of their respective dependencies.

3. Claims 8-14 and 26-31 are patentable under 35 U.S.C. 103(a) over Sudia. Claim 8 recites, a processor for generating a request that is generated upon initial power up of the apparatus, for configuration of the apparatus from a generic configuration to a selected or custom configuration which includes therein coded information for verification by the server of an identity of the apparatus, the coded information being generated using the cryptographic element, an interface for receiving information objects, corresponding to a predetermined feature set of the apparatus for configuring the apparatus, from the server through the communications network when the identity of the apparatus is verified by the server, the information objects modifying the generic configuration of the apparatus and a loader for directing the information objects to be loaded in the memory in accordance with a predetermined plan.

The Examiner notes that "Sudia does not specifically teach a loader for directing the information objects to be loaded in the memory in accordance with a predetermined plan". The Examiner argues that it would have been obvious for one skilled in the art to combine a loader for directing information objects to be loaded in a memory in accordance with a predetermined plan with Sudia.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the

14

art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). (MPEP § 2142).

Sudia does not disclose or suggest all the features of claim 8. Claim 8 specifically recites, a processor for generating a request that is generated upon initial power up of the apparatus, for configuration of the apparatus from a generic configuration to a selected or custom configuration. Claim 8 further recites information objects, corresponding to a predetermined feature set of the apparatus for configuring the apparatus, . . ., the information objects modifying the generic configuration of the apparatus. Sudia discloses a trusted device with an input-output interface or subsystem to assist in handling the flow of data commands to and from the microprocessor (Col. 13, L. 49-51) and that the trusted device can upgrade or supplement manufacturer embedded firmware (Col. 39, L. 7-9). Nowhere does Sudia disclose the trusted device making a request that is generated upon initial power up of the apparatus nonetheless a request for configuration of the apparatus from a generic configuration to a selected or custom configuration. Sudia only discloses that the trusted device does the upgrading or supplementing by accepting as input a body of data containing new or additional firmware code (Col. 39, L. 7-20). Further, Sudia does not disclose the modification of a generic configuration of the trusted device or any type of plan for loading objects into the trusted device. Sudia merely discloses that the permanent and non-modifiable
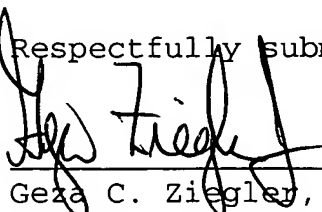
15

memory space [of the chip] contains data and firmware embedded into the chip during manufacturing (Col. 16, L. 14-16) and that the firmware can be upgraded or supplemented and nothing more. Therefore, a *prima facie* case of obviousness has not been established because Sudia fails to disclose or suggest all the limitation of claim 8. Thus claim 8 is patentable over Sudia.

Claim 26 is patentable over Sudia for reasons similar to those described above with respect to claim 8. Claims 9-14 and 27-31 are patentable over Sudia by reason of their respective dependencies.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Gera C. Ziegler, Jr.
Reg. No. 44,004

24 JANUARY 2006

Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

16

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date indicated below as first class mail in an envelope addressed to the Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: _Jan. 24, 2006_   Signature: _Meagleen Bayle_
                                    Person Making Deposit

17